Adentro Overview

Adentro provides consumers with an amazing WiFi experience at their favorite spots, while helping to grow local businesses by better engaging and targeting their customers. By offering a branded captive portal for your guest WiFi network, customers are given the ability to opt-in to targeted messaging sent using the Adentro platform.

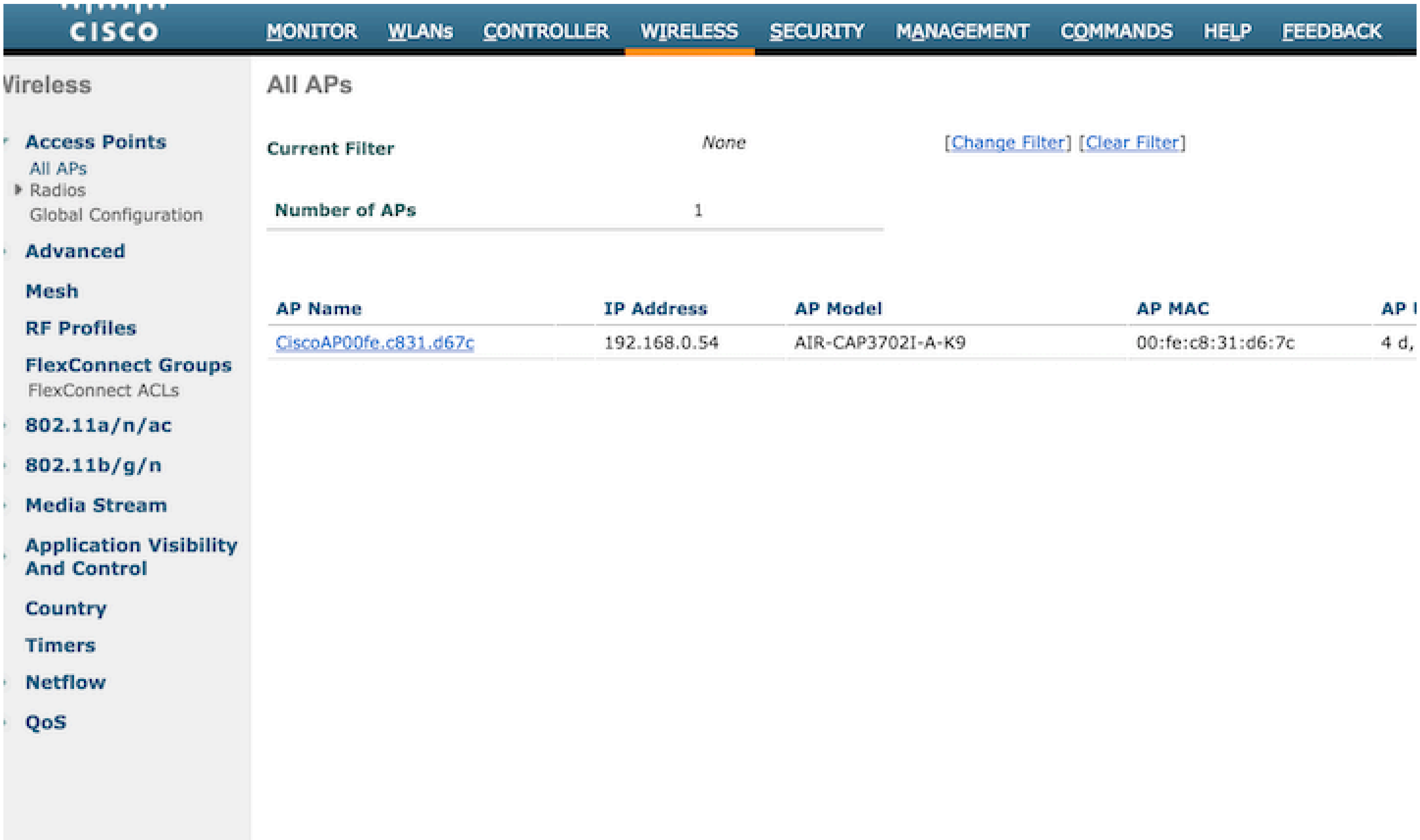
Adentro Configuration

This document provides basic details necessary for configuring a Cisco Wireless LAN Controller with the Adentro captive portal.

Note: This guide is not compatible with Cisco WAP series APs or EWC.

Identifying Cisco Access Points

Adentro identifies Cisco access points by their wireless MAC address. This can be retrieved via the WLC's UI. Adentro requires the **Base Radio MAC** for each access point that the guest wifi will operate on. The Base Radio MAC can be located in the AP details page under WIRELESS - All APs.

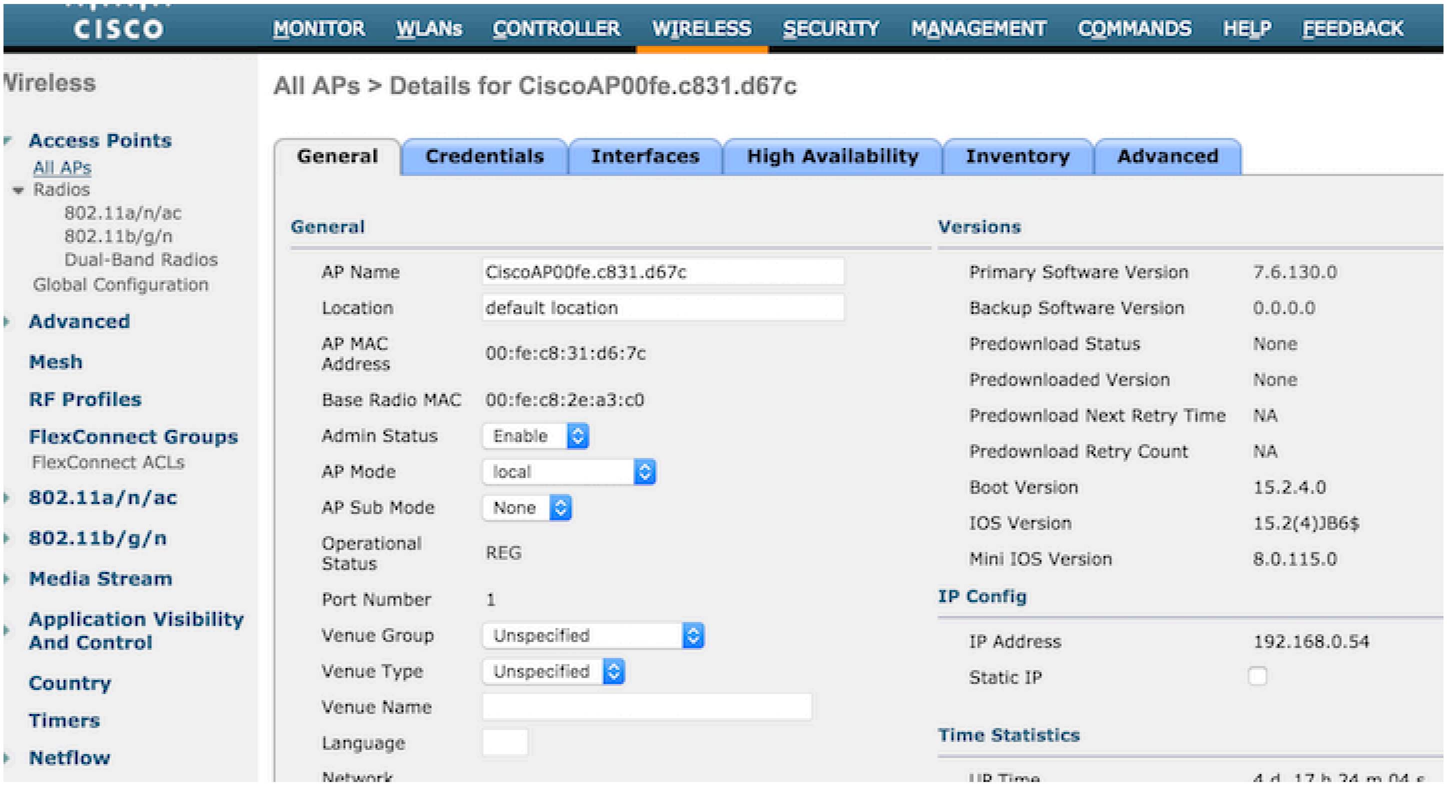


All APs

Current Filter None

Number of APs 1

AP Name	IP Address	AP Model	AP MAC	AP I
CiscoAP00fe.c831.d67c	192.168.0.54	AIR-CAP3702I-A-K9	00:fe:c8:31:d6:7c	4 d,



All APs > Details for CiscoAP00fe.c831.d67c

General

AP Name	CiscoAP00fe.c831.d67c
Location	default location
AP MAC Address	00:fe:c8:31:d6:7c
Base Radio MAC	00:fe:c8:2e:a3:c0
Admin Status	Enable
AP Mode	local
AP Sub Mode	None
Operational Status	REG
Port Number	1
Venue Group	Unspecified
Venue Type	Unspecified
Venue Name	
Language	
Network	

Versions

Primary Software Version	7.6.130.0
Backup Software Version	0.0.0.0
Predownload Status	None
Predownloaded Version	None
Predownload Next Retry Time	NA
Predownload Retry Count	NA
Boot Version	15.2.4.0
IOS Version	15.2(4)JB6$
Mini IOS Version	8.0.115.0

IP Config

IP Address	192.168.0.54
Static IP	□

Time Statistics

UP Time	4 d, 17 h 24 m 04 s

Create Pre-Authentication ACL

The pre-authentication ACL should allow access to all Adentro portal servers as well as your DNS and DHCP servers.

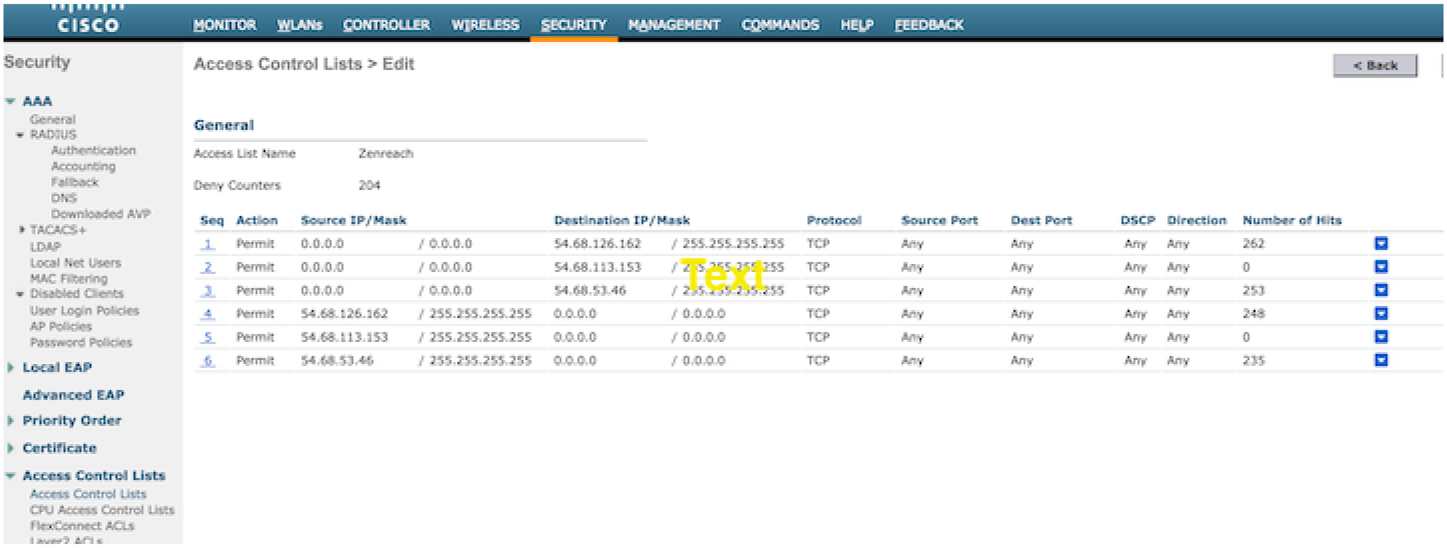
HTTP and HTTPS access must be permitted to the following IP addresses for gateway.wifast.com:

54.68.53.46

54.68.126.162

54.68.113.153

54.214.242.30



Access Control Lists > Edit

General

Access List Name	Zenreach
Deny Counters	204

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0	/ 0.0.0.0	54.68.126.162	/ 255.255.255.255	TCP	Any	Any	Any	Any	262
2	Permit	0.0.0.0	/ 0.0.0.0	54.68.113.153	/ 255.255.255.255	TCP	Any	Any	Any	Any	0
3	Permit	0.0.0.0	/ 0.0.0.0	54.68.53.46	/ 255.255.255.255	TCP	Any	Any	Any	Any	253
4	Permit	54.68.126.162	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	Any	Any	Any	Any	248
5	Permit	54.68.113.153	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	Any	Any	Any	Any	0
6	Permit	54.68.53.46	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	Any	Any	Any	Any	235

RADIUS Configuration

The guide linked above configures the controller to use local authentication. You must instead add the Adentro RADIUS servers as AAA auth and accounting servers and configure the WLAN to use them.

RADIUS Authentication

Step 1: In the left pane, expand **AAA**, then **RADIUS**, then click **Authentication**.

Step 2: Set **Auth Called Station ID Type** to **AP MAC Address**.

Step 3: Set **MAC Delimiter** to **Colon**.

Step 4: Click **New**.

Step 5: Enter the information in the tables below.

Step 6: Click **Apply**.

Step 7: Repeat steps 3-5 for the second table.

Server IP Address: 54.69.8.147

Shared Secret Format: ASCII

Shared Secret: 8fc40973252c42e196489d4a16849ff8

Confirm Shared Secret: 8fc40973252c42e196489d4a16849ff8

Port Number: 1812

Server Timeout: 5

Server IP Address: 54.68.29.80

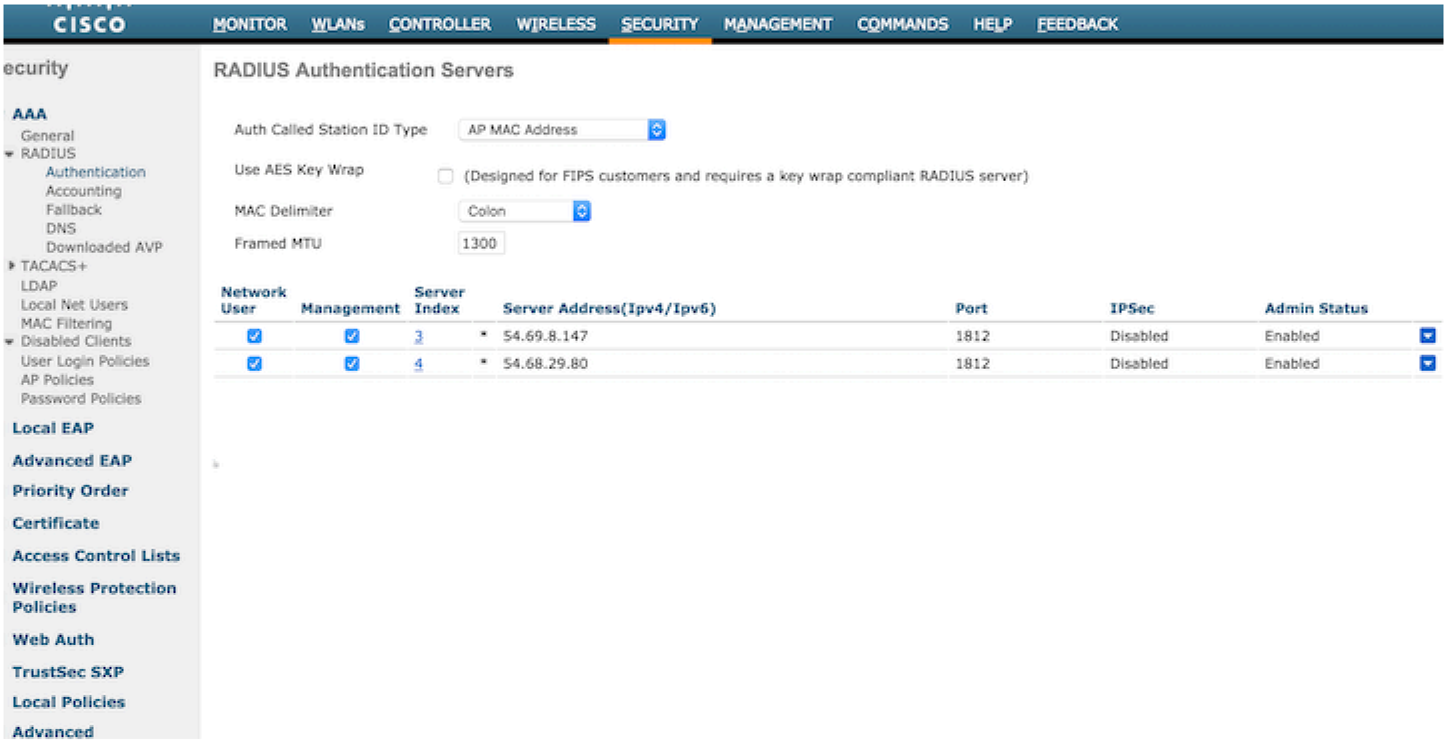
Shared Secret Format: ASCII

Shared Secret: 8fc40973252c42e196489d4a16849ff8

Confirm Shared Secret: 8fc40973252c42e196489d4a16849ff8

Port Number: 1812

Server Timeout: 5



RADIUS Authentication Servers

Auth Called Station ID Type	AP MAC Address
Use AES Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Delimiter	Colon
Framed MTU	1300

Network User	Management	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	☑	3	* 54.69.8.147	1812	Disabled	Enabled
☑	☑	4	* 54.68.29.80	1812	Disabled	Enabled

RADIUS Accounting

Use the same settings as above, but change the port to 1813 for each server.

RADIUS Configuration

Step 1: Open the **WLANs** page.

Step 2: Click **WLANs** in the left pane, and select the WLAN you want to edit.

Step 3: Click the **Security tab**.

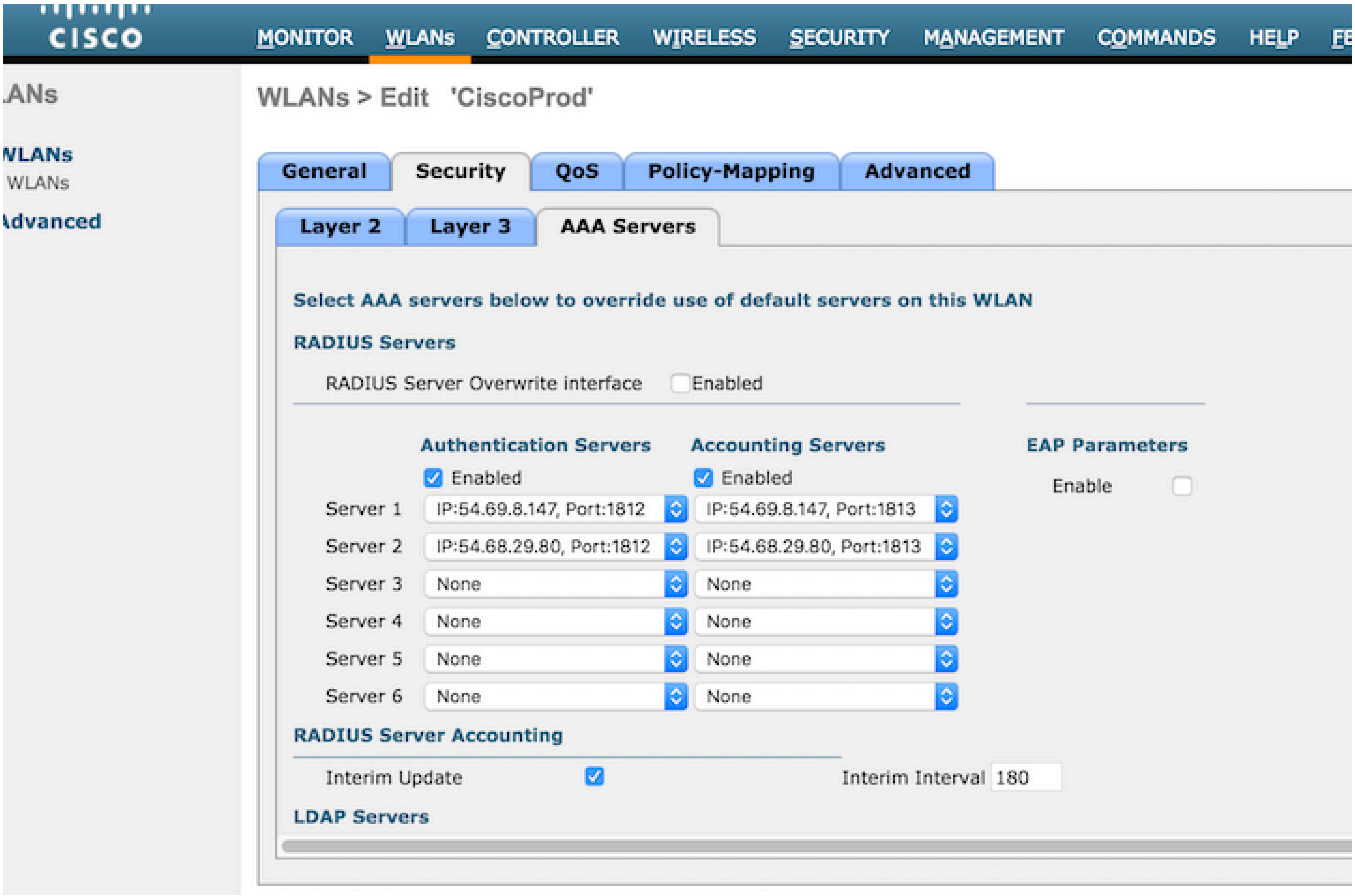
Step 4: Click the **AAA Servers** tab.

Step 5: Check the **Enabled checkboxes for Authentication Servers** and **Accounting Servers.**

Step 6: **Add** the two servers that were just set up under **Authentication Servers** and **Accounting Servers**.

Step 7: Check the **Interim Update** checkbox.

Step 8: Set **Interim Interval to 180**.



WLANs > Edit 'CiscoProd'

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
	☑ Enabled	☑ Enabled	Enable □
Server 1	IP:54.69.8.147, Port:1812	IP:54.69.8.147, Port:1813	
Server 2	IP:54.68.29.80, Port:1812	IP:54.68.29.80, Port:1813	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

RADIUS Server Accounting

Interim Update ☑ Interim Interval 180

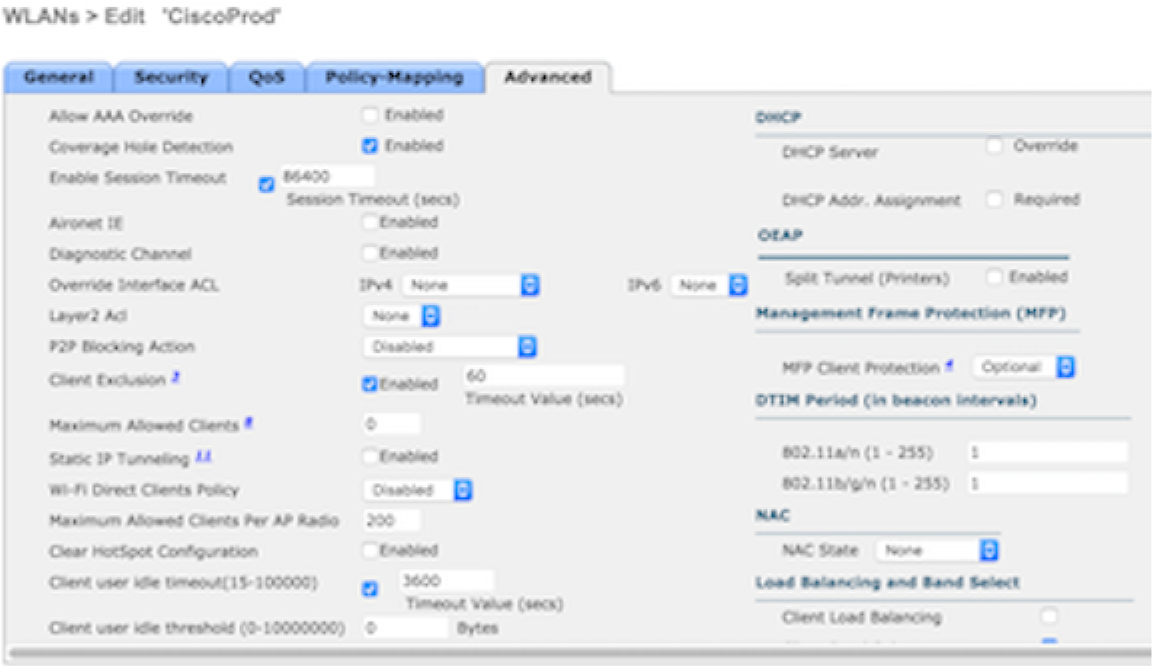
LDAP Servers

Step 9: Click the **Advanced tab**.

Step 10: Check the **Enable Session Timeout checkbox** and enter a value of **86400 seconds (24 hours)**.

Step 11: Check the **Client User Idle Timeout checkbox** and enter a value of **3600 seconds (1 hour)**.

Step 12: Set **Client User Idle Threshold to 0 bytes**.



WLANs > Edit 'CiscoProd'

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 86400 Session Timeout (secs)
Aironet IE □ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
P2P Blocking Action Disabled
Client Exclusion ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 0
Static IP Tunneling □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration □ Enabled
Client user idle timeout(15-100000) ☑ 3600 Timeout Value (secs)
Client user idle threshold (0-10000000) 0 Bytes

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP
Split Tunnel (Printers) □ Enabled

Management Frame Protection (MFP)
MFP Client Protection Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State None

Load Balancing and Band Select
Client Load Balancing □

Step 13: Click **Apply.**

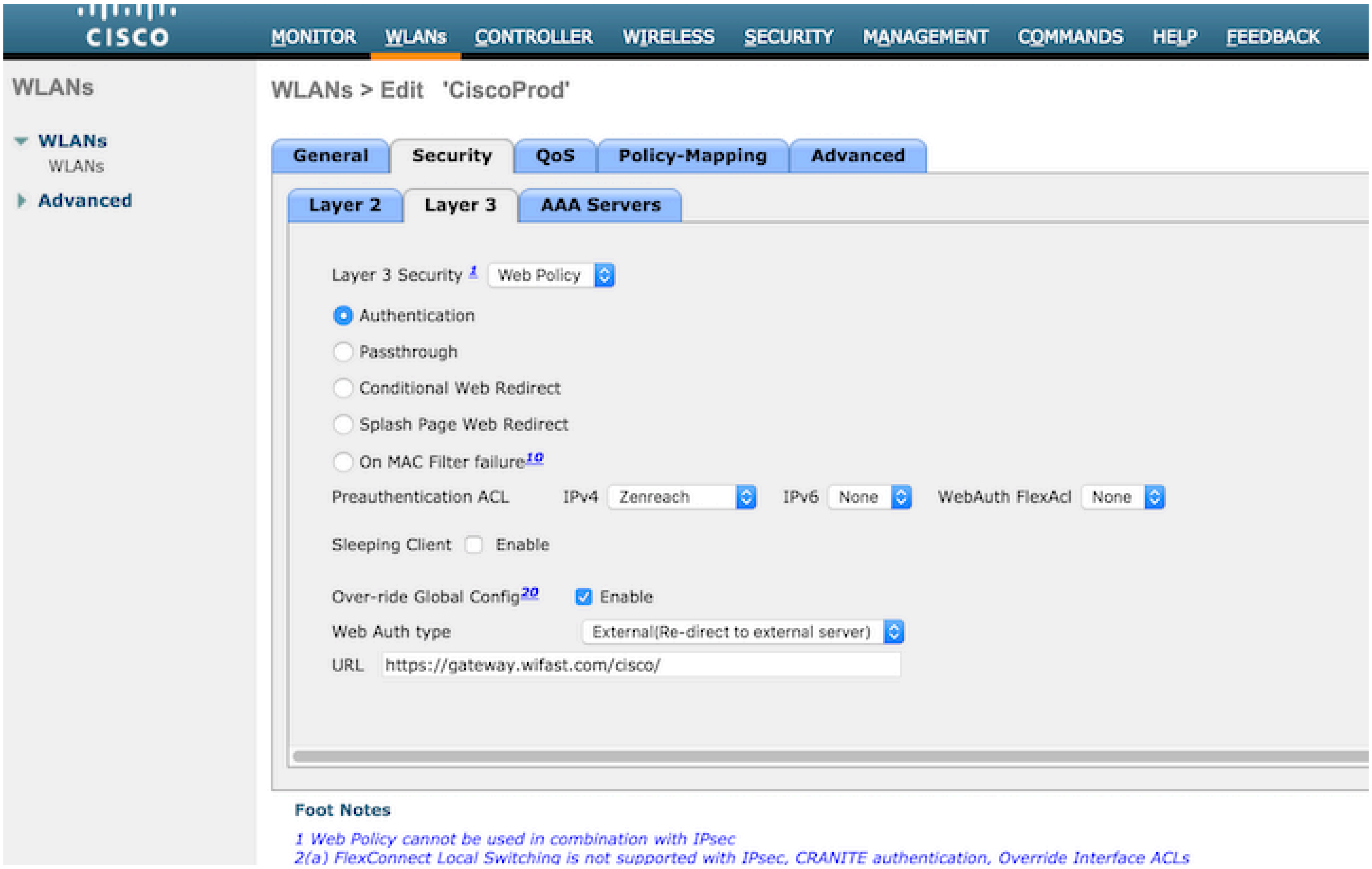
External Web Authentication

The WLC may have external web auth enabled globally or on a per-WLAN basis. In both cases the following External Webauth URL must be used:

https://gateway.wifast.com/cisco/

Remember to assign the Pre-Authentication ACL created previously to the WLAN.

The screenshot below shows the External Webauth URL set on a per-WLAN basis.



WLANs > Edit 'CiscoProd'

Layer 3 Security 1 Web Policy

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure10

Preauthentication ACL IPv4 Zenreach IPv6 None WebAuth FlexAcl None

Sleeping Client □ Enable

Over-ride Global Config20 ☑ Enable

Web Auth type External(Re-direct to external server)

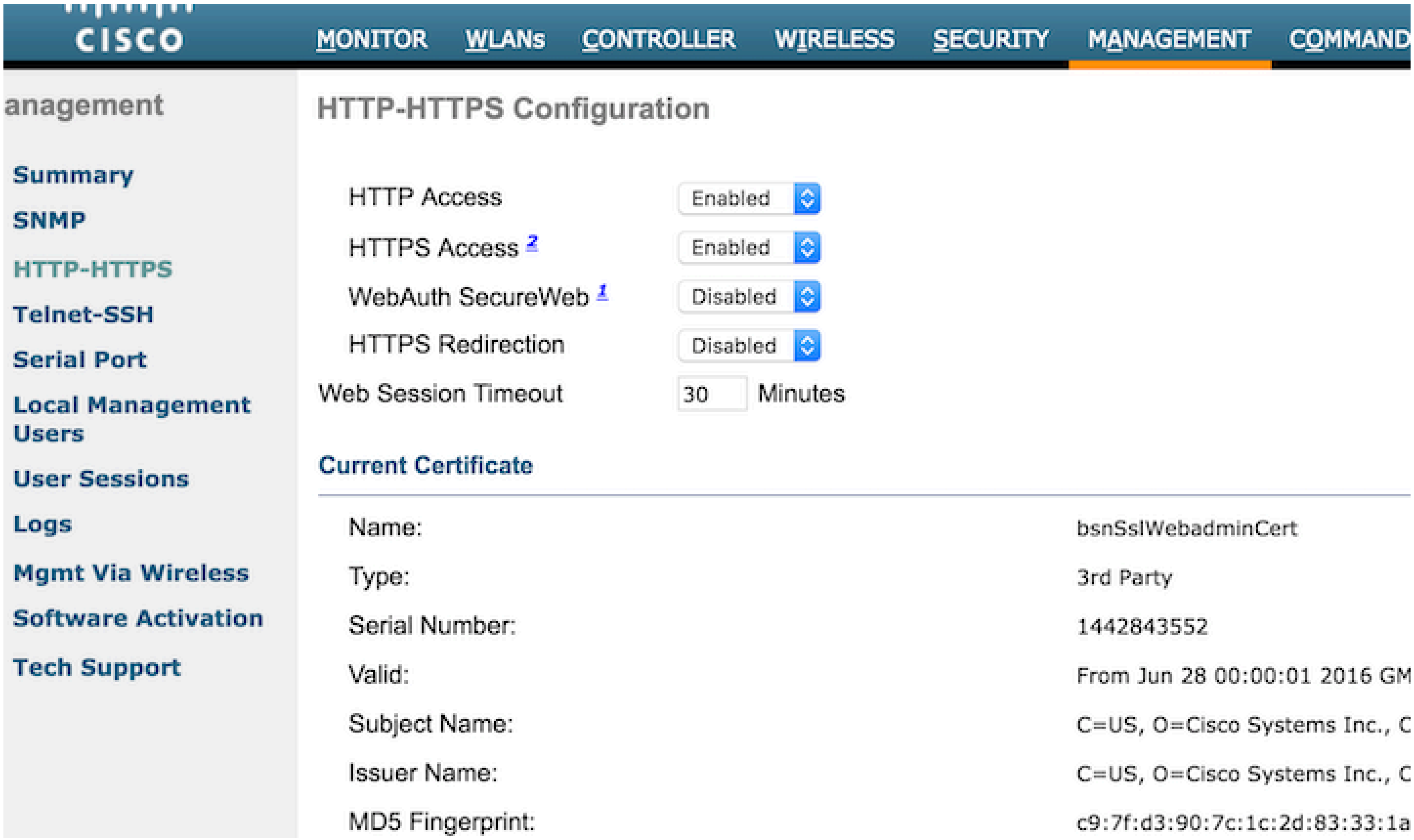
URL https://gateway.wifast.com/cisco/

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs

Disable WebAuth SecureWeb and HTTPS Redirection

Make sure the **WebAuth SecureWe**b and **HTTPS Redirection** (only present after firmware version 8.x) settings are disabled, otherwise after clicking the “Connect” button the user will be presented with a SSL error and will be unable to login. This can be resolved by disabling WebAuth SecureWeb and HTTPS Redirection on the controller.



HTTP-HTTPS Configuration

HTTP Access: Enabled

HTTPS Access [2]: Enabled

WebAuth SecureWeb [1]: Disabled

HTTPS Redirection: Disabled

Web Session Timeout: 30 Minutes

Current Certificate

Name: bsnSslWebadminCert

Type: 3rd Party

Serial Number: 1442843552

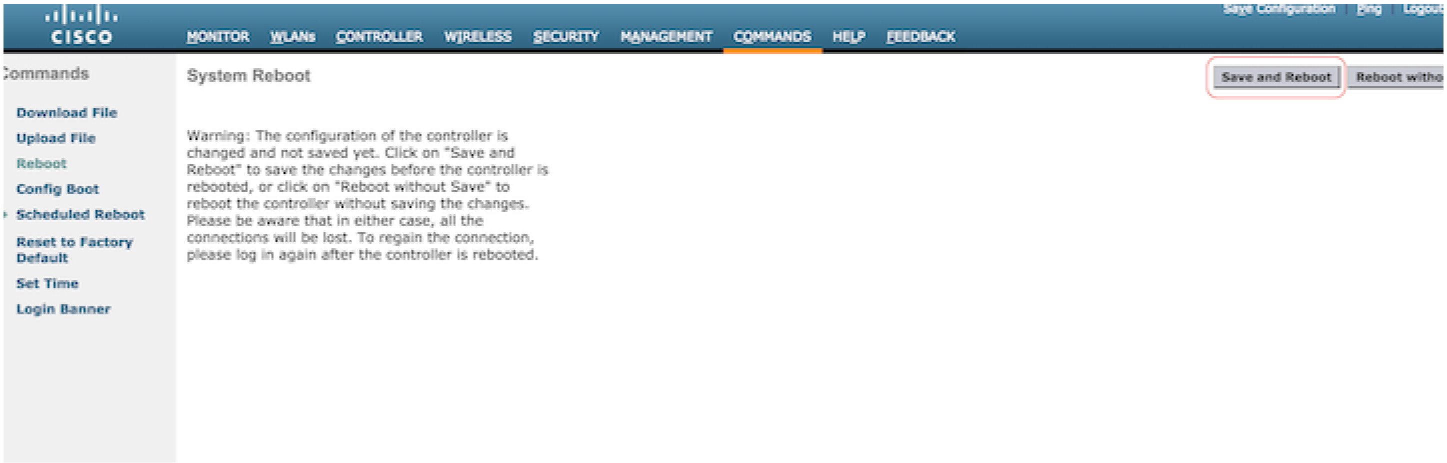
Valid: From Jun 28 00:00:01 2016 GM

Subject Name: C=US, O=Cisco Systems Inc., C

Issuer Name: C=US, O=Cisco Systems Inc., C

MD5 Fingerprint: c9:7f:d3:90:7c:1c:2d:83:33:1a

Make sure the configuration is saved and WLC rebooted after the configuration change.



System Reboot

Warning: The configuration of the controller is changed and not saved yet. Click on "Save and Reboot" to save the changes before the controller is rebooted, or click on "Reboot without Save" to reboot the controller without saving the changes. Please be aware that in either case, all the connections will be lost. To regain the connection, please log in again after the controller is rebooted.